Groups Containing a Given Number of Operators Whose Orders Are Powers of the Same Prime Number.

By G. A. Miller.

§ 1. *Introduction.*

Let G be any group whose order g is divisible by p^m but not by p^{m+1}, p being a prime number. A necessary and sufficient condition that G contains only one subgroup of order p^m is that the number of its operators whose orders are powers of p is exactly p^m. According to a theorem proved by Frobenius, the number of the distinct operators whose orders are powers of p, which are contained in G, is always divisible by p^m.* It is, however, not possible to construct a group in which this number is an arbitrary multiple of p^m. In fact, this number is at least p^{m+1} whenever it exceeds p^m, and it is at least $2\,p^{m+1} - p^m$ whenever it exceeds p^{m+1}, in accord with the theorems which we shall establish in what follows.

Let $H_1, H_2, \ldots, H_\lambda$ represent the totality of the subgroups of order p^m which are contained in G. It may happen that these subgroups have the property that all the operators which are common to one pair of them are common to every pair. On the other hand, it may happen that the operators which are common to one pair of such Sylow subgroups are not common to every pair of them. In what follows we shall be mainly concerned with the latter of these two possible cases, and we shall prove, in particular, that the number of these Sylow subgroups in the latter case must be at least $(p+1)^2$. That is, we shall prove that every possible pair of subgroups of order p^m contained in G has the same common operators whenever the number of these subgroups is less than $(p+1)^2$.

Suppose that H_1, H_2 have operators in common which are not common to every pair of the subgroups $H_1, H_2, \ldots, H_\lambda$. Let p^α be the largest number of common operators which can be found in any one of the possible pairs of these subgroups. All these subgroups may then be divided into sets characterized by the fact that each set is composed of all those which have the same

* Frobenius, *Berlin Sitzungsberichte*, 1895, p. 984.

p^α operators in common. It is evident that each of these sets is composed of the same number $1+kp$ of subgroups, since all the Sylow subgroups are conjugate under G. Moreover, no two of these sets can have more than one common subgroup of order p^m, since no pair of these Sylow subgroups can have more than p^α common operators.

The case which will interest us mostly in what follows is the one in which $k=1$. We may evidently assume that the two subgroups H_1, H_2 have p^α common operators. It also results that the subgroup K_1 constituted by these common operators is transformed into itself by exactly $p^{\alpha+1}$ operators of H_1 and by the same number of operators of each of the other p subgroups of order p^m which have K_1 in common. These $p^{\alpha+1}$ operators of any one of these subgroups clearly transform the other p subgroups of the same set among themselves.

Let $K_1, K_2, \ldots, K_\gamma$ be the conjugates of K_1 under H_1. It is clear that H_1 will transform the set of $p+1$ subgroups determined by H_1, H_2 into $\gamma = p^{m-\alpha-1}$ such sets, which have H_1 in common, and hence no two of these γ sets have any other subgroup of order p^m in common. If S is an operator of any one of these sets, which has the property that it transforms the common operators of this set into themselves but does not belong to H_1, then S can not transform the common operators of any other of these sets into themselves. In fact, if we assume that S transforms into themselves the common operators of two of these sets, it results that S and these common operators must generate a group which has more than p^α operators in common with H_1. Hence it follows that if we add the operators of each of these sets which do not belong to H_1 but transform the common operators of the set into themselves, we obtain

$$p^{m-\alpha}(p^{\alpha+1} - p^\alpha) = p^{m+1} - p^m$$

distinct operators.

In particular, when $\alpha = m-1$ it results that $\gamma = 1$, and all the operators of the set to which K_1 belongs must transform K_1 into itself. The total number of the distinct operators of the set must therefore be p^{m+1}. As a special case of this we may observe that when G contains exactly $p+1$ subgroups of order p^m, the number of its operators whose orders are powers of p must be exactly p^{m+1}, as is also directly evident. If $\alpha < m-1$, each set of $p+1$ subgroups evidently contains more than p^{m+1} distinct operators, and if $\alpha = m-1$ and there is more than one such set, G must again contain more than p^{m+1} operators whose orders are powers of p. Hence we have, as a special case of the given developments, that *a necessary and sufficient condition that a group whose order is divisible by p^m but not by p^{m+1} contains exactly $p+1$ subgroups of order p^m is that it contains exactly p^{m+1} operators whose orders are powers of p.*

§ 2. *Groups in Which the Common Operators of Some One Pair of Sylow Subgroups Are Common to Every Pair of Such Subgroups.*

If some two Sylow subgroups H_1, H_2 of order p^m have operators in common which are not common to every pair of subgroups of order p^m contained in G, there are evidently two cases to be considered. In the first of these cases every pair of Sylow subgroups of order p^m contained in G has the same number of common operators but the operators which are common to some one pair are not common to every pair. In the second case, G contains some pair of subgroups of order p^m which has more operators in common than some other pair.

We shall first prove that if every pair of subgroups of order p^m in G has p^{m-1} operators in common, each of these pairs must contain the same p^{m-1} operators. To prove this theorem it will be convenient to consider the group of transformations T of the Sylow subgroups of G. Since every pair of subgroups of order p^m in G has p^{m-1} operators in common, all the transitive constituents of the Sylow subgroups of order p^m in T are of degree p. The subgroup T_1, which is composed of all of the substitutions of T which omit a given letter, must therefore contain an invariant subgroup of order p^{m_1} whose transitive constituents are all of degree p, and the degree of T_1 must be kp, $kp+1$ being the degree of T.*

If all the substitutions of T_1, excluding the identity, were of degree kp, all the Sylow subgroups of order p^m in G would involve the same p^{m-1} operators. Hence we may assume that the invariant abelian subgroup of order p^{m_1} in T_1 involves a subgroup of a degree which is less than kp and of order p^{m_1-1}, $m_1 > 1$. This subgroup must be contained invariantly in at least $p+1$ subgroups of order p^{m_1} contained in T. As these groups of order p^{m_1} are abelian, the group generated by them must have a central which includes the given subgroup of order p^{m_1-1}. As this group would have an abelian constituent whose order is a power of p, and another constituent of degree $1+kp$ involving non-invariant subgroups whose orders are powers of p, it evidently could not be constructed, and hence we have proved the theorem: *If every possible pair of Sylow subgroups of order p^m in a given group has p^{m-1} operators in common, then all of these subgroups must have the same p^{m-1} operators in common.*

From this theorem it results directly that G must contain at least one pair of subgroups of order p^m which has less than p^{m-1} common operators whenever all the pairs of subgroups of order p^m in G do not have the same largest common

---

* American Journal of Mathematics, Vol. XXXII (1910), p. 299.

subgroup. The number of these subgroups in such a G must clearly exceed p^2. If this were not the case, these subgroups would be transformed according to a transitive substitution group T in which the subgroup T_1 would contain an invariant subgroup of order p^{m_1} whose transitive constituents would all be of degree p. As this subgroup would contain substitutions which would omit some of the letters of T_1, it results in exactly the same manner as in the preceding paragraph that such a T could not exist. This proves the lemma: *If any group contains less than* p^2+1 *Sylow subgroups of order* p^m, *every pair of these subgroups must contain the same common operators.*

When the Sylow subgroups of order p^m in G do not all contain the same largest common subgroup, they must occur in sets of $1+kp$ such that each set is composed of all those Sylow subgroups of order p^m which have the same largest subgroup in common. The order of the largest common subgroup for one set must be the same as the order of this subgroup in any other set, and k must have the same value for each of these sets since all the Sylow subgroups of G are conjugate under G. Any two of these sets have at most one subgroup of order p^m in common, for if two such sets would have two such subgroups in common these two subgroups would have more common operators than the order of the subgroups composed of all the operators which are common to such a set. As such a set can not be transformed into itself by any Sylow subgroup of order p^m unless this subgroup belongs to the set, it results that the number of these sets can not be less than $p+1$. Hence it results that the number of Sylow subgroups of order p^m in G can not be less than the sum of

$$p+1, \quad p, \quad p-1, \quad \ldots, \quad 1=\tfrac{1}{2}(p+1)(p+2)$$

unless all of these Sylow subgroups have the same largest subgroup in common. In the special case when $p=2$, this gives a larger limit than the one expressed in the preceding theorem, while it gives the same limit when $p=3$.

It is not difficult to prove that the lower limit for the number of Sylow subgroups, which was found in the preceding paragraph, is always too small. To prove this, it is only necessary to consider the cases when $p=2$ or 3, since the other cases are included in the theorem stated above. The case when $p=2$ may readily be disposed of, since the given formula gives an even number six, while the number of these subgroups is odd. In fact, the number of these subgroups could not be seven, since the groups of degree 7 which are groups of transformations of Sylow subgroups are contained in the matacyclic group of this degree, and hence the Sylow subgroup of order 2^{m_1} in T_1 is of order 2 and of degree 6. The case when $p=3$ is included in the more general lemma,

which we proceed to prove; viz., the number of Sylow subgroups of order p^m must exceed p^2+1 whenever some two of these subgroups have operators in common which are not common to all of them.

To prove this generalization of the lemma stated above, we shall prove that we arrive at an absurdity by assuming that G contains exactly p^2+1 Sylow subgroups of order p^m and that some two H_1, H_2 of these subgroups have operators in common which are not contained in all of them. We consider again the group of transformations T of these Sylow subgroups and observe that the only case which requires consideration is the one in which the invariant Sylow subgroup of order p^{m_1} in T_1 is transitive, T_1 being defined as before. This subgroup of order p^{m_1} must be non-regular, and hence it must contain an intransitive subgroup of order p^{m_1-2}, whose degree is less than p^2. This subgroup must occur in at least $p+1$ conjugates of T_1, and hence it is invariant in at least $p+1$ subgroups of order p^{m_1-1} contained in G. Just as in the cases considered above, it results that these subgroups of order p^{m_1-1} would generate a group which could not occur in T, and hence it results that *if a group contains no more than* p^2+1 *Sylow subgroups of order* p^m, *every pair of these subgroups must contain the same common operators.* This lemma will be useful to establish a more general result in what follows.

We are now in position to prove the theorem that the number of Sylow subgroups of order p^m in G must be at least equal to $(p+1)^2$, whenever the operators common to some two of these subgroups are not necessarily common to all of them. To prove this theorem by means of the two lemmas which have been established, it is only necessary to prove that the number of these subgroups could not be p^2+p+1. If this number were p^2+p+1, T_1 would have two transitive constituents of degrees p^2 and p respectively. If a transitive subgroup of the former would correspond to the identity of the latter, this transitive subgroup would be invariant under $p+1$ conjugates of T_1. These conjugates would generate an intransitive group with two transitive constituents of degrees p^2 and $p+1$ respectively. The latter would clearly be at least doubly transitive. Hence T would be imprimitive, since T_1 could not be maximal, and a system of imprimitivity would involve $p+1$ letters. This is impossible, since p^2+p+1 is not divisible by $p+1$.

If the subgroup which would correspond to the identity of the constituent of degree p in T_1 were intransitive, this would be the only subgroup of this order and degree contained in T_1, since the remaining substitutions of the constituent of degree p^2 would involve all the letters of this constituent. Hence the given subgroup would again be invariant under $p+1$ conjugates of T_1,

and T would be imprimitive. Just as in the preceding case, there would be a system of imprimitivity of degree $p+1$, while this is not a divisor of the degree of T. Hence we have established the theorem: *If any group contains less than* $(p+1)^2$ *Sylow subgroups of order* p^m, *then all the operators which are common to some two of these subgroups are necessarily common to all of them.*

To give an instance where G contains exactly $(p+1)^2$ Sylow subgroups of order p^m which are such that the operators common to some two of these subgroups are not common to all of them, we may consider the Sylow subgroups of order 4 in the direct product of two non-cylic groups of order 6. This direct product clearly contains nine subgroups of order 4; and one of these subgroups has two operators in common with each of four others, while it has only the identity in common with each of the remaining four. The total number of distinct operators which are contained in these nine subgroups is clearly sixteen. The transitive group of degree 6 and of order 72 furnishes another instance of a group which contains exactly $(p+1)^2$ Sylow subgroups of order p^m having the property that some two of these subgroups have operators in common which are not common to all of them.

§ 3. *Groups Which Contain a Small Number of Operators Whose Orders Are Powers of a Given Prime Number.*

We shall again assume that the order of G is divisible by p^m but not by p^{m+1}, p being a prime. For every pair of values for p and m, m being any positive integer, there is evidently at least one group G which contains exactly $p+1$ Sylow subgroups of order p^m. It has been observed that a necessary and sufficient condition that G contains exactly $p+1$ Sylow subgroups of order p^m is that the number of its operators whose orders are powers of p is exactly p^{m+1}. We proceed to find a lower limit for the number of such operators in G when G contains more than $p+1$ such subgroups.

If all the operators which are common to two subgroups of order p^m in G are necessarily common to all of its subgroups of this order, it is evident that the number of such operators contained in G can not be less than

$$(2p+1)(p^m - p^{m-1}) + p^{m-1} = 2p^{m+1} - p^m.$$

We proceed to consider the cases when G contains at least two Sylow subgroups H_1, H_2 of order p^m whose common operators do not occur in all of its other Sylow subgroups of this order, and we begin with the case when G contains at least one Sylow subgroup of order p^m which has p^{m-1} operators in

common with H_1. Hence G contains at least $p+1$ such subgroups. If it had more than $p+1$ such subgroups, they would contain at least $2\,p^{m+1}-p^m$ distinct operators. Hence we shall assume that G contains exactly $p+1$ Sylow subgroups having p^{m-1} operators in common with H_1.

The Sylow subgroups of order p^m contained in G must therefore occur in sets of $p+1$ such that each set is characterized by the fact that it is composed of all these subgroups which have a certain set of p^{m-1} operators in common. Two such sets have at most one subgroup in common. If they have no subgroup in common, the number of these sets is at least $p+1$, since G contains at least $(p+1)^2$ subgroups of order p^m. If they have a common subgroup, the number of these sets must be at least $2\,(p+1)$, since each of these subgroups must occur at least twice among the sets. We shall first consider the latter case.

The $p+1$ subgroups of order p^m which constitute such a set must generate a group K_1 which involves exactly p^{m+1} operators whose orders are powers of p in accord with the theorem proved above. Let K_2 be a conjugate of K_1 under G and suppose that H_1 is common to K_1 and K_2. If S is any operator of K_1 which is not included in H_1, then S can not occur in K_2. For, if S would also occur in K_2, it would transform into themselves two subgroups of order p^{m-1} contained in H_1, and hence it would transform H_1 into itself. It would therefore be contained in H_1, but this is contrary to the hypothesis. Hence K_2 contains exactly $p\,(p^m-p^{m-1})=p^{m+1}-p^m$ operators which are not found in K_1, and the total number of distinct operators in K_1 and K_2 is $2\,p^{m+1}-p^m$.

If K_3 is another conjugate of K_1, but is not identical with K_1 or K_2, it can not have more than p^m operators in common with either one of the two subgroups K_1, K_2. As it has the identity in common with both of these, and as it involves p^{m+1} distinct operators, it results that K_3 must involve at least one operator which is distinct from the operators contained in K_1 and K_2. Hence it follows that G must contain at least $2\,p^{m+1}-p^m+p^m=2\,p^{m+1}$ operators whose orders are powers of p whenever it satisfies the two conditions that the operators which are common to some two of its Sylow subgroups of order p^m are not common to all of these subgroups and that a Sylow subgroup is found in more than one set of $p+1$ subgroups having p^{m-1} common operators. This lower limit is exactly attained in the direct product of two symmetric groups of order 6.

If all the subgroups of order p^m in G are contained in sets of $p+1$, which have p^{m-1} operators in common, and if no such subgroup is common to two such sets, then each of these sets generates a subgroup which has one and only one

transitive constituent of degree p. Let K_1, K_2 represent two such subgroups. As the transitive constituents of degree $p+1$ in K_1, K_2 can not have any letter in common whenever G is the group of transformations of its Sylow subgroups of order p^m, it results that a subgroup of order p^m in K_1 can not have more than p^{m-2} operators in common with K_2, since these common operators would transform the transitive constituents of degrees $p+1$ in K_1 and K_2 into themselves, and hence they would omit a letter of a transitive constituent of degree p^α, $\alpha > 1$, in this Sylow subgroup of order p^m. Hence the $p+1$ Sylow subgroups of order p^m in K_1 can not have more than $(p+1)\,p^{m-2}$ operators in common with K_2. That is, G would again have at least $2\,p^{m+1}$ distinct operators whose orders are powers of p, since the number of these operators is divisible by p^m and must exceed $2\,p^m - p^m$. Since this result is true when G is the group of transformations of its own Sylow subgroups of order p^m, it evidently holds true in all cases.

We have now considered the possible cases when both of the following conditions are satisfied: G contains at least two Sylow subgroups of order p^m whose common operators are not common to all of its subgroups of this order, and there are at least two subgroups of order p^m in G which have p^{m-1} common operators. We proceed to consider the cases when the former but not the latter of these two conditions is fulfilled. Two of the Sylow subgroups of order p^m in G can therefore not have more than p^{m-2} common operators. We may divide all the subgroups of order p^m in G into sets which are such that each set is composed of all these subgroups which have a maximal number p^α of common operators.

Let H_1 be one of such a set of subgroups. If its subgroup of order p^α, which is common to all the subgroups of the set, is invariant under $p^{\alpha+\beta}$ operators of H_1, the set will be composed of $p^\beta+1$ subgroups of order p^m and these will involve $(p^\beta+1)\,(p^m - p^\alpha) + p^\alpha = p^{m+\beta} + p^m - p^{\alpha+\beta}$ distinct operators. This is at least as large as $2\,p^{m+1}$ when $\beta > 1$. Hence we may restrict our attention to the case when each of the given sets involves exactly $p+1$ subgroups of order p^m having p^α common operators, and hence we must assume $\beta = 1$ for all the possible sets.

Consider two of these sets of $p+1$ subgroups which have H_1 in common, and which have been so chosen that the two subgroups of order p^α, which are respectively common to all the Sylow subgroups of each of the two separate sets, have $p^{\alpha-1}$ common operators. Let S be any operator which occurs in each of these two sets but is not contained in H_1. The two subgroups of order p^m to which S belongs must therefore have S and the given $p^{\alpha-1}$ operators in

common. Hence the subgroup formed by these $p^{\alpha-1}$ operators must be invariant under S, and the group generated by S and this subgroup is of order p^{α}. This proves that all the operators of one of these subgroups of order p^m, besides H_1, which are common to both of the two sets under consideration, must form a group.

The order of this group is less than p^m; for, if it were p^m this Sylow group would involve an invariant subgroup of order p^{α} which would also appear in another Sylow subgroup of this order, since the given subgroup of order $p^{\alpha-1}$ would be invariant under the former of these two Sylow subgroups. Hence each Sylow subgroup, besides H_1, of one of these sets of $p+1$ subgroups must contain at least $p^m - p^{m-1}$ operators which do not appear in the other set. Hence the two sets contain at least

$$p^{m+1} - p^m + p^{m+1} + p^m - p^{\alpha+1} = 2\,p^{m+1} - p^{\alpha+1}$$

distinct operators. Hence G contains at least $2\,p^{m+1}$ distinct operators whose orders are powers of p in this case.

If two Sylow subgroups of order p^m have p^{α} common operators and these constitute a non-invariant subgroup, the set composed of all the subgroups which have these p^{α} operators in common is transformed by any subgroup of such a set into another set having another set of p^{α} operators in common, but having the transforming subgroup in common with the first set. Hence we have completed a proof of the theorem: *If a group whose order is divisible by p^m but not by p^{m+1} contains exactly $2\,p^{m+1} - p^m$ operators whose orders are powers of p, it involves exactly $2\,p+1$ subgroups of order p^m and all of these involve the same p^{m-1} operators.*

UNIVERSITY OF ILLINOIS.